

IN THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of the claims in the application:

1. (Currently amended) A method for controlling access to digital information, comprising:

encrypting said digital information using a data encrypting key;

modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key;

encrypting said location-modified data encrypting key using a key encrypting key ~~and information derived from a location identity attribute that defines at least a specific geographic location~~ to produce an encrypted location-modified data encrypting key; and

~~associating communicating~~ said encrypted location-modified data encrypting key ~~with and~~ said encrypted digital information to a recipient device such that said encrypted digital information can be ~~accessed~~ decrypted by the recipient only at said specific geographic location.

2. (Currently amended) The method of Claim 1, wherein said location identity ~~attribute~~ data further comprises at least a location value and a proximity value of said specific geographic location.

3. (Currently amended) The method of Claim 2, wherein said location value ~~corresponds to~~ defines a location of an intended receiver of said digital information.

4. (Original) The method of Claim 2, wherein said location value further comprises at least one of a latitude, longitude, altitude and time dimension.

5. (Currently amended) The method of Claim 2, wherein said location value identify data further ~~comprises~~ defines a universal location that encompasses the entire earth.

6. (Original) The method of Claim 3, wherein said proximity value corresponds to a zone that encompasses said location.

7. (Cancelled)

8. (Original) The method of Claim 1, further comprising identifying location of a receiver at which access to said digital information is sought.

9. (Original) The method of Claim 8, wherein said location identifying step further comprises recovering said location from a GPS receiver.

10. (Currently amended) The method of Claim 1, wherein ~~said information derived from~~ said location identity attribute data further comprises a location value and a shape parameter, the shape parameter defining a shape of a region encompassing the specific geographic location.

11. (Currently amended) The method of Claim 1, further comprising:  
    decrypting said encrypted location-modified data ~~encryption~~  
    encrypting key using a key decrypting key;  
    and using a location value to recover said data encrypting key from  
    said location-modified data encrypting key; and  
    decrypting said digital information using said ~~data encryption~~  
    encrypting key.

12. (Currently amended) The method of Claim 11, further comprising deriving said location value from a signal received by a GPS receiver and a shape parameter defining a shape of a region encompassing the specific geographic location.

13. (Original) The method of Claim 1, wherein said digital information further comprises a secret key, and further comprising the step of distributing said secret key to an intended receiver.

14. (Currently amended) The method of Claim 11, further comprising ~~rendering unusable~~ precluding decryption of said encrypted digital information if said step of decrypting said encrypted digital information is attempted at other than said specific geographic location.

15. (Currently amended) The method of Claim 11, further comprising ~~rendering unusable~~ precluding decryption of said encrypted digital information if said step of decrypting said encrypted digital information is attempted without using said key decrypting key.

16. (Original) The method of Claim 1, further comprising routing said encrypted digital information to an intended receiver through at least one distributor.

17. (Original) The method of Claim 16, wherein said routing step further comprises adding a layer of encryption of said data encrypting key for said at least one distributor.

18. (Currently amended) The method of Claim 1, further comprising generating said data ~~encryption~~ encrypting key using a pseudo-random number generator.

19. (Currently amended) The method of Claim 18, wherein said step of generating said ~~encryption~~ data encrypting key further comprises using GPS signals to partially seed said pseudo-random number generator.

20. (Currently amended) The method of Claim 1, further comprising decrypting and recovering said data encrypting key from said encrypted location-modified data encrypting key using a key decrypting key and a location value, and re-encrypting said data encrypting key using at least one of a different location identity attribute data and a different key encrypting key to produce a different encrypted location-modified data encrypting key.

21. (Original) The method of Claim 1, further comprising providing a key table used to store a plurality of keys including said key encrypting key.

22. (Original) The method of Claim 21, further comprising associating said plurality of keys with respective providers of said digital information.

23. (Original) The method of Claim 21, further comprising administering management of said plurality of keys in said key table.

24. (Original) The method of Claim 23, wherein said administering step further comprises adding, changing or deleting any one of said plurality of keys in said key table.

25. (Original) The method of Claim 23, wherein said key table is located with a remote device, and said administering step further comprises adding, changing or deleting any one of said plurality of keys in said key table remotely.

26. (Original) The method of Claim 25, wherein said administering step further comprises including a signature when adding, changing or deleting any one of said plurality of secret keys in said key table.

27. (Original) The method of Claim 21, wherein said step of providing a key table further comprises storing keys used for signing data and validating signatures.

28. (Currently amended) An apparatus for controlling access to digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

encrypting said digital information using a data encrypting key;

modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key;

encrypting said location-modified data encrypting key using a key encrypting key and ~~information derived from a location identity attribute that defines at least a specific geographic location~~ to produce an encrypted location-modified data encrypting key; and

associating communicating said encrypted location-modified data encrypting key with and said encrypted digital information to a recipient device such that said encrypted digital information can be accessed decrypted by the recipient only at said specific geographic location.

29. (Currently amended) The apparatus of Claim 28, wherein said location identity ~~attribute~~ data comprises at least a location value and a proximity value of said specific geographic location.

30. (Currently amended) The apparatus of Claim 29, wherein said location value ~~corresponds to~~ defines a location of an intended receiver of said digital information.

31. (Original) The apparatus of Claim 29, wherein said location value further comprises at least one of a latitude, longitude, altitude and time dimension.

32. (Original) The apparatus of Claim 29, wherein said proximity value corresponds to a zone that encompasses said location.

33. (Cancelled)

34. (Original) The apparatus of Claim 28, wherein said processor is further operable to identify location of a receiver at which access to said digital information is sought.

35. (Original) The apparatus of Claim 28, further comprising a GPS receiver coupled to said processor.

36. (Currently amended) The apparatus of Claim 28, wherein ~~said information derived from~~ said location identity attribute data further comprises a location value and a shape parameter, the shape parameter defining a shape of a region encompassing said specific geographic location.

37. (Original) The apparatus of Claim 28, wherein said digital information further comprises a secret key, and said processor is further operable to distribute said secret key to an intended receiver located at said specific geographic location.

38. (Original) The apparatus of Claim 28, wherein said processor is further operable to route said encrypted digital information to an intended receiver through at least one distributor.

39. (Original) The apparatus of Claim 28, further comprising a pseudo-random number generator operatively coupled to said processor to generate said data encrypting key.

40. (Currently amended) The apparatus of Claim 28, wherein said processor is further operable to decrypt said encrypted location-modified data encrypting key, and re-encrypt said location-modified data encrypting key using at least one of a different location identity ~~attribute~~ data and a different key encrypting key.

41. (Original) The apparatus of Claim 28, wherein said memory further comprises a key table used to store a plurality of keys including said key encrypting key.

42. (Original) The apparatus of Claim 41, wherein ones of said plurality of keys are associated with respective providers of said digital information.

43. (Original) The apparatus of Claim 41, wherein processor is further operable to add, change or delete any one of said plurality of keys in said key table.

44. (Original) The method of Claim 41, wherein said processor is further operable to provide a signature for authentication of one of said plurality of keys.

45. (Currently amended) An apparatus for receiving digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

receiving encrypted digital information and an encrypted location-modified data encrypting key;

decrypting said encrypted location-modified data encrypting key using a key encrypting key to obtain a location-modified data encrypting key;

determining a location value that defines a specific geographic location of said apparatus;

extracting a data encrypting key from said location-modified data encrypting key using said location value; and

~~decrypting said data encrypting key using a key decrypting key and a location identity attribute that defines a specific geographic location of said apparatus;~~  
and

decrypting said encrypted digital information using said ~~decrypted~~ data encrypting key.

46. (Currently amended) The apparatus of Claim 45, wherein said function of decrypting said encrypted digital information further comprises ~~rendering unusable~~ precluding decryption of said encrypted digital information if decryption is attempted at other than said specific geographic location.

47. (Original) The apparatus of Claim 45, further comprising a GPS receiver coupled to said processor.



48. (Currently amended) The apparatus of Claim 45, wherein said processor is further operable to re-encrypt said data encrypting key using at least one of a different location identity ~~attribute~~ data and a different key encrypting key.

49. (Original) The apparatus of Claim 45, wherein said memory further comprises a key table used to store a plurality of keys including said key decrypting key.

50. (Original) The apparatus of Claim 45, wherein ones of said plurality of keys are associated with respective providers of said digital information.